


[Home](#) | [Login](#) | [Logout](#) | [Account Information](#) | [About](#) | [Feedback](#)

Welcome United States Patent and Trademark Office

[Search Results](#)
[BROWSE](#)
[SEARCH](#)
[IEEE Xplore GUIDE](#)

Results for "((('smart card' &lt;and&gt; 'private key' &lt;and&gt; pin)&lt;in&gt;metadata)"

Your search matched 1 of 1745737 documents.

A maximum of 100 results are displayed. 25 to a page, sorted by Relevance in Descending order.


[Search Options](#)
[View Session History](#)
[New Search](#)
[Key](#)

IEEE JNL	IEEE Journal or Magazine
IET JNL	IET Journal or Magazine
IEEE CONF	IEEE Conference Proceeding
IEE CFP	IEE Conference Proceeding
IEEE STD	IEEE Standard

Modify Search

((('smart card' &lt;and&gt; 'private key' &lt;and&gt; pin)&lt;in&gt;metadata)

[Search](#)
☐ Check to search only within this results set

Display Format:



Citation



Citation &amp; Abstract

[IEEE/IEE](#)
[Books](#)
[Educational Courses](#)

IEEE/IEE Journals, transactions, letters, magazines, conference proceedings, and standards.

[view selected items](#)
[Select All](#) [Deselect All](#)

1. A Smart Card Mediated Mobile Platform for Secure E-Mail Communication  
 Kardas, Geylan; Celikal, Ebru;  
 Information Technology, 2007. ITNG '07. Fourth International Conference on  
 2-4 April 2007 Page(s):925 - 928  
 Digital Object Identifier 10.1109/ITNG.2007.21  
[AbstractPlus](#) | [Full Text: PDF\(144 KB\)](#) [IEEE CONF](#)  
[Rights and Permissions](#)

powered by


[Help](#) [Contact](#)

© Copyright


[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)

 Search: ☒ The ACM Digital Library ☐ The Guide  
 ('smart and card' and 'private and key' and PIN)

**THE ACM DIGITAL LIBRARY**

Feedback

('smart and card' and 'private and key' and PIN)

Published before December 2005

Found 58 of

Terms used: 'smart card' 'private key' PIN

Sort results by relevance

Save results to a Binder

 Refine these results with [Advanced Search](#)

Display results expanded form

☐ Open results in a new window
Try this search in [The ACM Guide](#)

Results 1 - 20 of 58

Result page: 1 2 3 [next](#) >>

### 1 [Smart Cards and Biometrics: The cool way to make secure transactions](#)

 David Corcoran, David Sims, Bob Hillhouse  
 March 1999 Linux Journal, Volume 1999 Issue 59es  
 Publisher: Specialized Systems Consultants, Inc.
Full text available: [html\(22.95 KB\)](#) Additional Information: [full citation](#), [index terms](#)

Ads by Google

[Publisher Files](#)  
[Easily Make & i](#)  
[PDF Files Adob](#)  
[Compliant. Inst](#)  
[Download!](#)  
[Creative Commons](#)

### 2 [Muscle Flexes Smart Cards into Linux](#)

 David Corcoran  
 August 1998 Linux Journal, Volume 1998 Issue 52es  
 Publisher: Specialized Systems Consultants, Inc.
Full text available: [html\(16.89 KB\)](#) Additional Information: [full citation](#), [abstract](#), [index terms](#)

The newest kind of card for your pocketbook offers better security for the information it holds

[ISBN Numbers](#)  
[Publishers](#)  
[ISBN & Barcode](#)  
[at \\$55. Contact](#)  
[ISBN's in Minut](#)  
[www.isbn-us.com](#)

### 3 [Power consumption profile analysis for security attack simulation in smart cards at high abstraction level](#)

 K. Rothbart, U. Neffe, Ch. Steger, R. Weiss, E. Rieger, A. Muehlberger  
 September 2005 EMSOFT '05: Proceedings of the 5th ACM international conference on Embedded software

Publisher: ACM

Full text available: [pdf\(273.40 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)
[Bar/Pub. POS](#)  
[Complete POS](#)  
[For Any Bar Or](#)  
[Unbeatable Pri](#)  
[www.papayash.com](#)

Smart cards are embedded systems which are used in an increasing number of secure applications. As they store and deal with confidential and secret data many attacks are performed on these cards to reveal this private information. Consequently, the security ...

Key words: SystemC, analysis, attack, embedded security, fault injection, power profile, simulation, smart card


[GIS Image](#)  
[Segmentation](#)  
[Shapfiles from](#)  
[imagery Wizard](#)  
[segment, classi](#)  
[image5img.com](#)

#### 4 [Distributed PIN verification scheme for improving security of mobile devices](#)

Jian Tang, Vagan Terziyan, Jari Veijalainen

April 2003 Mobile Networks and Applications. Volume 8 Issue 2

Publisher: Kluwer Academic Publishers

Full text available:  [pdf\(298.43 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#)

The main driving force for the rapid acceptance rate of small sized mobile devices is the capability to perform e-commerce transactions at any time and at any place, especially while on the move. There are, however, also weaknesses of this type of e-commerce, ...

Key words: measure, mobile device, probability, risks, security, uncover


#### 5 [Who's got the key?](#)



David Henry

November 1999 SIGUCCS '99: Proceedings of the 27th annual ACM SIGUCCS conference on User services: Mile high expectations

Publisher: ACM

Full text available:  [pdf\(30.32 KB\)](#) Additional Information: [full citation](#), [references](#), [index terms](#)

Key words: PKI, certificate authority, encryption

#### 6 [Design of a scalable RSA and ECC crypto-processor](#)



Ming-Cheng Sun, Chih-Pin Su, Chih-Tsun Huang, Cheng-Wen Wu

January 2003 ASPDAC: Proceedings of the 2003 conference on Asia South Pacific design automation

Publisher: ACM

Full text available:  [pdf\(127.33 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#)

In this paper, we propose a scalable word-based crypto-processor that performs modular multiplication based on modified Montgomery algorithm for finite fields  $GF(P)$  and  $GF(2^m)$ . The unified crypto-processor supports scalable ...


#### 7 [Some facets of complexity theory and cryptography: A five-lecture tutorial](#)



Jörg Rothe

December 2002 ACM Computing Surveys (CSUR). Volume 34 Issue 4

Publisher: ACM

Full text available:  [pdf\(2.78 MB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#), [review](#)

In this tutorial, selected topics of cryptology and of computational complexity theory are presented. We give a brief overview of the history and the foundations of classical cryptography, and then move on to modern public-key cryptography. Particular ...

Key words: Complexity theory, interactive proof systems, one-way functions, public-key cryptography, zero-knowledge protocols

#### 8 [Anonymous E-prescriptions](#)

Giuseppe Ateniese, Breno de Medeiros



November 2002 WPES '02: Proceedings of the 2002 ACM workshop on Privacy in the Electronic Society

Publisher: ACM

Full text available: pdf(304.10 KB) Additional Information: full citation, abstract, references

This paper studies issues related to privacy protection of medical data, arguing that the topic is suitable for applied cryptographic research. We present the problem of medicine prescription privacy and describe a practical system that employs standard ...

**Keyw ords:** medical information privacy, privacy-preserving cryptographic techniques, public-key cryptography

9

Taking the best from a company history - designing with interaction styles



Trond Are Øritsland, Jacob Buur

August 2000 DIS '00: Proceedings of the 3rd conference on Designing interactive systems: processes, practices, methods, and techniques

Publisher: ACM

Full text available: pdf(1.49 MB) Additional Information: full citation, abstract, references, cited by, index terms

In architecture and industrial design, the concept of style plays a major role in education as a way of explaining the historical inheritance and comparing alternative design expressions. In this article we claim that interaction design can benefit greatly ...

**Keyw ords:** interaction design, interaction style, quality in use, solid user interface

10

Zero-interaction authentication



Mark D. Corner, Brian D. Noble

September 2002 MobiCom '02: Proceedings of the 8th annual international conference on Mobile computing and networking

Publisher: ACM

Full text available: pdf(273.30 KB) Additional Information: full citation, abstract, references, cited by, index terms

Laptops are vulnerable to theft, greatly increasing the likelihood of exposing sensitive files. Unfortunately, storing data in a cryptographic file system does not fully address this problem. Such systems ask the user to imbue them with long-term authority ...

**Keyw ords:** cryptographic file systems, mobile computing, stackable file systems, transient authentication

11

Security wrappers and power analysis for SoC technologies



C. H. Gebotys, Y. Zhang

October 2003 CODES+ISSS '03: Proceedings of the 1st IEEE/ACM/IFIP international conference on Hardware/software codesign and system synthesis

Publisher: ACM

Full text available: pdf(790.57 KB) Additional Information: full citation, abstract, references, cited by, index terms

Future wireless internet enabled devices will be increasingly powerful supporting

many more applications including one of the most crucial, security. Although SoCs offer more resistance to bus probing attacks, power/EM attacks on cores and network snooping ...

**Key words:** VLIW, adiabatic, design, performance, security

## 12 Using GSM to enhance e-commerce security



Vorapraee Khu-smith, Chris J. Mitchell

September 2002 WMC '02: Proceedings of the 2nd international workshop on Mobile commerce

Publisher: ACM

Full text available: pdf(177.48 KB) **Additional Information:** [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#)

Today, an e-commerce transaction is typically protected using SSL/TLS@. However, there remain some risks in such use of SSL/TLS@. These include that of information being stored in clear at the end point of the communication link and lack of user authentication. ...

**Key words:** E-commerce security, GSM security, mobile or Internet payment protocol

## 13 Current mask generation: a transistor level security against DPA attacks



Daniel Mesquita, Jean-Denis Techer, Lionel Torres, Gilles Sassatelli, Gaston Cambon, Michel Robert, Fernando Moraes

September 2005 SBCCI '05: Proceedings of the 18th annual symposium on Integrated circuits and system design

Publisher: ACM

Full text available: pdf(513.86 KB) **Additional Information:** [full citation](#), [abstract](#), [references](#), [index terms](#)

The physical implementation of cryptographic algorithms may leak to some attacker security information by the side channel data, as power consumption, timing, temperature or electromagnetic emanation. The Differential Power Analysis (DPA) is a powerful ...

**Key words:** DPA, countermeasures, cryptography, side channel attacks

## 14 Adapting globus and kerberos for a secure ASCII grid



Patrick C. Moore, Wilbur R. Johnson, Richard J. Detry

November 2001 Supercomputing '01: Proceedings of the 2001 ACM/IEEE conference on Supercomputing (CDROM)

Publisher: ACM

Full text available: pdf(143.26 KB) **Additional Information:** [full citation](#), [abstract](#), [references](#), [index terms](#)

Porting a complex secure application from one security infrastructure to another is often difficult or impractical. Grid security associated with the Globus toolkit is supported by a Grid Security Infrastructure (GSI) based on a Public Key Infrastructure ...

**Key words:** ASCII, GSSAPI, globus, grid, kerberos, security

15 [Untraceable RFID tags via insubvertible encryption](#)

Giuseppe Ateniese, Jan Camenisch, Breno de Medeiros

November 2005 CCS '05: Proceedings of the 12th ACM conference on Computer and communications security

Publisher: ACM

Full text available: pdf(238.38 KB) Additional Information: full citation, abstract, references, cited by, index terms

We introduce a new cryptographic primitive, called *insubvertible encryption*, that produces ciphertexts which can be randomized without the need of any key material. Unlike plain universal re-encryption schemes, insubvertible encryption prevents ...

Key words: RFID privacy, bilinear maps, universal re-encryption

16 [Requirements traceability in automated test generation: application to smart card software validation](#)

F. Bouquet, E. Jaffuel, B. Legeard, F. Peureux, M. Utting

May 2005 A-MOST '05: Proceedings of the 1st international workshop on Advances in model-based testing

Publisher: ACM

Full text available: pdf(665.74 KB) Additional Information: full citation, abstract, references, index terms

Automated test case and test driver generation from a formal model is becoming a more widely used practice in the smart card area. This innovative approach for validation testing makes it possible to ensure the functional coverage of the test suite and ...

Key words: formal model, model-based testing, requirements traceability

17 [A Low Device Occupation IP to Implement Rijndael Algorithm](#)

Alex Panato, Marcelo Barcelos, Ricardo Reis

March 2003 DATE '03: Proceedings of the conference on Design, Automation and Test in Europe: Designers' Forum - Volume 2. Volume 2

Publisher: IEEE Computer Society

Full text available: pdf(465.66 KB) Publisher Site Additional Information: full citation, abstract, index terms

This work presents a soft IP description of Rijndael, the Advanced Encryption Standard (AES) of National Institute of Standards and Technology (NIST). This Rijndael implementation run its symmetric cipher algorithm using a key size of 128 bits, mode ...

18 [Security on FPGAs: State-of-the-art implementations and attacks](#)

Thomas Wollinger, Jorge Guajardo, Christof Paar

August 2004 ACM Transactions on Embedded Computing Systems (TECS). Volume 3 Issue 3

Publisher: ACM

Full text available: pdf(296.79 KB) Additional Information: full citation, abstract, references, index terms

In the last decade, it has become apparent that embedded systems are integral

parts of our every day lives. The wireless nature of many embedded applications as well as their omnipresence has made the need for security and privacy preserving mechanisms ...


**Keyw ords:** Cryptography, FPGA, attacks, cryptographic applications, reconfigurable hardware, reverse engineering, security

19 [Spy-resistant keyboard: more secure password entry on public touch screen displays](#)

Desney S. Tan, Pedram Keyani, Mary Czerwinski

November 2005 OZCHI '05: Proceedings of the 19th conference of the computer-human interaction special interest group (CHISIG) of Australia on Computer-human interaction: citizens online: considerations for today and the future


Publisher: Computer-Human Interaction Special Interest Group (CHISIG) of Australia

Full text available:  [pdf\(454.44 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#)

Current software interfaces for entering text on touch screen devices mimic existing mechanisms such as keyboard typing or handwriting. These techniques are poor for entering private text such as passwords since they allow observers to decipher what ...


**Keyw ords:** input technique, keyboard, password, selective attention, touch screen, visual search

20 [A context-related authorization and access control method based on RBAC:](#)

 Marc Wilkens, Simone Feriti, Alberto Sanna, Marcelo Masera

June 2002 SACMAT '02: Proceedings of the seventh ACM symposium on Access control models and technologies

Publisher: ACM

Full text available:  [pdf\(260.70 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#)

This paper describes an application of authorization and access control based on the Role Based Access Control (RBAC) method and integrated in a comprehensive trust infrastructure of a health care application. The method is applied to a health care business ...

**Keyw ords:** role based access control (RBAC), secure health care system, trust infrastructure

Results 1 - 20 of 58

Result page: 1 2 3 [next](#) [>>](#)

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2008 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  Adobe Acrobat  QuickTime  Windows Media Player  Real Player


[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)

 Search: ☒ The ACM Digital Library ☐ The Guide  
 ('smart and card' and 'private and key' and PIN)

**THE ACM DIGITAL LIBRARY**

Feedback

 ('smart and card' and 'private and key' and PIN)  
 Published before December 2005  
 Terms used: 'smart card' 'private key' PIN

Found 58 of 231

Sort results by relevance

Save results to a Binder

 Refine these results with [Advanced Search](#)

Display results expanded form

☐ Open results in a new window
Try this search in [The ACM Guide](#)

Results 21 - 40 of 58

Result page: &lt;&lt; previous 1 2 3 next &gt;&gt;

## 21 [Protected transmission of biometric user authentication data for oncard-matching](#)

Add by Google


 Ulrich Waldmann, Dirk Scheuermann, Claudia Eckert  
 March 2004 SAC '04: Proceedings of the 2004 ACM symposium on Applied computing  
 Publisher: ACM

Full text available: pdf(574.45 KB) Additional Information: full citation, abstract, references, cited by

Since fingerprint data are no secrets but of public nature, the verification data transmitted to a smartcard for oncard-matching need protection by appropriate means in order to assure data origin in the biometric sensor and to prevent bypassing the ...

Key words: authentication, biometrics, cryptographic protocols, data integrity, electronic signature, oncard-matching, smartcards, system security, tamper proof environment

 Online Payments  
 \$25 sign up bonus  
 Transactions among  
 accountholders. Try  
 Now!  
[www.1ststop.com](#)

 eCommerce Webs  
 Design  
 Focusing on Big  
 Business Websites  
 Award-Winning Design  
 \$10K Minimum.  
[www.AwardWebsites.com](#)

## 22 [Secure scan: a design-for-test architecture for crypto chips](#)


 Bo Yang, Kaijie Wu, Ramesh Karri  
 June 2005 DAC '05: Proceedings of the 42nd annual conference on Design automation  
 Publisher: ACM

Full text available: pdf(234.65 KB) Additional Information: full citation, abstract, references, index terms

Scan-based Design-for-Test (DFT) is a powerful testing scheme, but it can be used to retrieve the secrets stored in a crypto chip thus compromising its ...

Key words: crypto hardware, scan-based DFT, security, testability

 eCommerce for  
 Dynamics GP  
 Integrated B2B, B2C  
 Sales Portal Expand  
 your business, full  
 service  
[www.dyn.com](#)

 Buy Area E-Comm  
 Set Your Business  
 With E-Commerce  
 Unique to Your  
 Products!  
[www.dyn.com](#)

## 23 [On-line e-wallet system with decentralized credential keepers](#)

 Stig Frode Mjølhus, Chunming Rong  
 February 2003 Mobile Networks and Applications, Volume 8 Issue 1  
 Publisher: Kluwer Academic Publishers

Full text available: pdf(240.23 KB) Additional Information: full citation, abstract, references, cited by



by, index terms

We propose a generalization of the architecture of an electronic wallet, as first developed in the seminal European research project CAFE. With this model you can leave most of the content of your electronic wallet at the security of your residential ...


**Keyw ord s:** digital credentials, e-wallet architecture, mobile commerce, payment protocols, privacy

## 24 Planning for code buffer management in distributed virtual execution environments

Shukang Zhou, Bruce R. Childers, Mary Lou Soffa

June 2005 VEE '05: Proceedings of the 1st ACM/USENIX international conference on Virtual execution environments

Publisher: ACM

Full text available:  pdf(216.28 KB) **Additional Information:** full citation, abstract, references, cited by, index terms

Virtual execution environments have become increasingly useful in system implementation, with dynamic translation techniques being an important component for performance-critical systems. Many devices have exceptionally tight performance and memory constraints ...


**Keyw ord s:** adaptive code cache, code buffer, distributed environments, dynamic translation, generational cache, program partitioning

## 25 Shake them up!: a movement-based pairing protocol for CPU-constrained devices

Claude Castelluccia, Pars Mutaf

June 2005 MobiSys '05: Proceedings of the 3rd international conference on Mobile systems, applications, and services

Publisher: ACM

Full text available:  pdf(295.02 KB) **Additional Information:** full citation, abstract, references, cited by, index terms


This paper presents a new pairing protocol that allows two CPU-constrained wireless devices Alice and Bob to establish a shared secret at a very low cost. To our knowledge, this is the first software pairing scheme that does not rely on expensive public-key ...

## 26 A simple mechanism for capturing and replaying wireless channels

Glenn Judd, Peter Steenkiste

August 2005 E-WIND '05: Proceeding of the 2005 ACM SIGCOMM workshop on Experimental approaches to wireless network design and analysis

Publisher: ACM

Full text available:  pdf(6.06 MB) **Additional Information:** full citation, abstract, references, cited by, index terms

Physical layer wireless network emulation has the potential to be a powerful experimental tool. An important challenge in physical emulation, and traditional simulation, is to accurately model the wireless channel. In this paper we examine the possibility ...


Keywords: channel capture, emulation, wireless

## 27 [Protecting file systems with transient authentication](#)

Mark D. Corner, Brian D. Noble

January 2005 *Wireless Networks*, Volume 11 Issue 1-2

Publisher: Kluwer Academic Publishers

Full text available:  [pdf\(422.63 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)


Laptops are vulnerable to theft, greatly increasing the likelihood of exposing sensitive files. Unfortunately, storing data in a cryptographic file system does not fully address this problem. Such systems ask the user to imbue them with long-term authority ...

## 28 [Requirements traceability in automated test generation: application to smart card software validation](#)

F. Bouquet, E. Jaffuel, B. Legeard, F. Peureux, M. Utting

July 2005 *ACM SIGSOFT Software Engineering Notes*, Volume 30 Issue 4

Publisher: ACM

Full text available:  [pdf\(665.74 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Automated test case and test driver generation from a formal model is becoming a more widely used practice in the smart card area. This innovative approach for validation testing makes it possible to ensure the functional coverage of the test suite and ...


Keywords: formal model, model-based testing, requirements traceability

## 29 [At home with the technology: an ethnographic study of a set-top-box trial](#)

Jon O'Brien, Tom Rodden, Mark Rouncefield, John Hughes

September 1999 *ACM Transactions on Computer-Human Interaction* (TOCHI), Volume 6 Issue 3

Publisher: ACM

Full text available:  [pdf\(438.27 KB\)](#) Additional Information: [full citation](#), [references](#), [cited by](#), [index terms](#), [review](#)



Keywords: coordination and collaboration, domestic environment, ethnography, evaluation, interactive devices

## 30 [Business: The 8th layer: Will the digital signature transform e-commerce?](#)

Kate Gerwig

September 2000 *netWorker*, Volume 4 Issue 3

Publisher: ACM

Full text available:  [pdf\(502.72 KB\)](#);  [html\(13.80 KB\)](#) Additional Information: [full citation](#), [index terms](#)

Current flattening in software and hardware for security applications

Radu Muresan, Catherine Gebotys

September 2004 CODES+ ISSS '04: Proceedings of the 2nd IEEE/ACM/IFIP international conference on Hardware/software codesign and system synthesis

Publisher: ACM

Full text available: pdf(344.68 KB) Additional Information: full citation, abstract, references, index terms

This paper presents a new current flattening technique applicable in software and hardware. This technique is important in embedded cryptosystems since power analysis attacks (that make use of the current variation dependency on data and program) compromise ...

Keyw ords: current flattening, hardware architecture, power analysis attacks

32 Report of the national workshop on internet voting: issues and research agenda

C. D. Mote, Jr.

May 2002 dg.o '02: Proceedings of the 2002 annual national conference on Digital government research

Publisher: Digital Government Research Center

Full text available: pdf(539.99 KB) Additional Information: full citation

33 Defending wireless infrastructure against the challenge of DDoS attacks

Xianjun Geng, Yun Huang, Andrew B. Whinston

June 2002 Mobile Networks and Applications, Volume 7 Issue 3

Publisher: Kluwer Academic Publishers

Full text available: pdf(313.57 KB) Additional Information: full citation, abstract, references, cited by, index terms

This paper addresses possible Distributed Denial-of-Service (DDoS) attacks toward the wireless Internet including the Wireless Extended Internet, the Wireless Portal Network, and the Wireless Ad Hoc network. We propose a conceptual model for defending ...

Keyw ords: DDoS attack, PBN, wireless ad hoc network, wireless extended internet, wireless infrastructure, wireless portal network

34 Software security and privacy risks in mobile e-commerce

Anup K. Ghosh, Tara M. Swaminatha

February 2001 Communications of the ACM, Volume 44 Issue 2

Publisher: ACM

Full text available: pdf(90.58 KB) html(38.81 KB) Additional Information: full citation, appendices and supplements, references, cited by, index terms

35 [A smartcard for authentication in WLANs](#)

Marc Loutrel, Pascal Urien, Guy Pujolle

October 2003 LANC '03: Proceedings of the 2003 IFIP/ACM Latin America conference on Towards a Latin American agenda for network research

Publisher: ACM

Full text available: [pdf\(333.05 KB\)](#)Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Wireless LANs based on the IEEE 802.11b standard have spread very quickly over the past few years. Nevertheless a lot of security issues remain and stop its deployment in corporations. One of the most important issues is the authentication of a terminal ...

Keyw ords: authentication, smartcard, wireless LANs

36 [The blocker tag: selective blocking of RFID tags for consumer privacy](#)

Ari Juels, Ronald L. Rivest, Michael Szydlo

October 2003 CCS '03: Proceedings of the 10th ACM conference on Computer and communications security

Publisher: ACM

Full text available: [pdf\(223.05 KB\)](#)Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#)

We propose the use of "selective blocking" by "blocker tags" as a way of protecting consumers from unwanted scanning of RFID tags attached to items they may be carrying or wearing. While an ordinary RFID tag is a simple, cheap (e.g. five-cent) passive ...

Keyw ords: RFID tags, barcodes, privacy, tree walking

37 [Consumer perceptions of privacy, security and trust in ubiquitous commerce](#)

George Roussos, Theano Moussouri

November 2004 Personal and Ubiquitous Computing, Volume 8 Issue 6

Publisher: Springer-Verlag

Full text available: [pdf\(378.27 KB\)](#)Additional Information: [full citation](#), [abstract](#), [cited by](#), [index terms](#)

Commerce is a rapidly emerging application area of ubiquitous computing. In this paper, we discuss the market forces that make the deployment of ubiquitous commerce infrastructures a priority for grocery retailing. We then proceed to report on a study ...

38 [Payments and banking with mobile personal devices](#)

Amir Herzberg

May 2003 Communications of the ACM, Volume 46 Issue 5

Publisher: ACM

Full text available: [pdf\(152.82 KB\)](#) [html\(21.60 KB\)](#)Additional Information: [full citation](#),
[abstract](#),  
[references](#), [cited by](#), [index terms](#),  
[review](#)

Mobile devices enable secure, convenient authorization of e-banking, retail payment, brokerage, and other types of transactions.

39 [Securing wireless data: system architecture challenges](#)



Srivaths Ravi, Anand Raghunathan, Nachiketh Potlapally

October 2002 | SSS '02: Proceedings of the 15th international symposium on System Synthesis

Publisher: ACM

Full text available: [pdf\(172.35 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#)

Security is critical to a wide range of current and future wireless data applications and services. This paper highlights the challenges posed by the need for security during system architecture design for wireless handsets, and provides an overview ...

Key words: 3DES, AES, DES, IPSec, RSA, SSL, WTLS, decryption, design methodology, embedded system, encryption, handset, mobile computing, performance, platform, security, security processing, system architecture, wireless communications

40 [Secure internet access to SAP's R-3: keeping dragons out](#)

Katherine Jones

May 1998 International Journal of Network Management, Volume 8 Issue 3

Publisher: John Wiley & Sons, Inc.

Full text available: [pdf\(187.01 KB\)](#) Additional Information: [full citation](#), [abstract](#), [index terms](#)

The security of the networking environment is critical for today's corporations. Issues such as reliably identifying remote-access users, checking authorizations, data-transfer security and database security are of paramount importance. This article ...

Results 21 - 40 of 58

Result page: [<<](#) [previous](#) [1](#) [2](#) [3](#) [next](#) [>>](#)

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2008 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads: [Adobe Acrobat](#) [QuickTime](#) [Windows Media Player](#) [Real Player](#)


[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)

 Search: The ACM Digital Library The Guide  
 ('smart and card' and 'private and key' and PIN)


USPTO

THE ACM DIGITAL LIBRARY

Feedback

('smart and card' and 'private and key' and PIN)

Published before December 2005

Terms used: 'smart card' 'private key' PIN

Found 58

Sort results by relevance

Save results to a Binder

 Refine these results with [Advanced Search](#)

Display results expanded form

☐ Open results in a new window
Try this search in [The ACM Guide](#)

Results 41 - 58 of 58

Result page: [<<](#) [previous](#) [1](#) [2](#) [3](#)41 [Projectors: advanced graphics and vision techniques](#)

Ads by Google

 Ramesh Raskar  
 August 2004 SIGGRAPH '04: ACM SIGGRAPH 2004 Course Notes  
 Publisher: ACM  
 Full text available: pdf(6.53 MB) [Additional Information: full citation, cited by](#)

 Free MATLAB  
 CD include:  
 Demos, prc  
 reference e  
 more.  
[www.mathworks.com](http://www.mathworks.com)
42 [Statistics and secret leakage](#)
 Jean-Sebastien Coron, David Naccache, Paul Kocher  
 August 2004 ACM Transactions on Embedded Computing Systems (TECS), Volume 3 Issue 3  
 Publisher: ACM

 Full text available: pdf(218.95 KB) [Additional Information: full citation, abstract, references, cited by, index terms](#)

In addition to its usual complexity assumptions, cryptography silently assumes that information can be physically protected in a single location. As one can easily imagine, real-life devices are not ideal and information may leak through different physical ...

Keyw ords: Cryptography, side-channel analysis

[Dijkstra's / White Paper Build software converged \[PDF\]](#)  
[www.cdnlab.org](http://www.cdnlab.org)
43 [Information-rich commerce at a crossroads: business and technology adoption requirements](#)
[Matching 5 Fastest, m matching s B2C, Entitle](#)  
[www.cdnlab.org](http://www.cdnlab.org)

 Robert G. Fichman, Mary J. Cronin  
 September 2003 Communications of the ACM, Volume 46 Issue 9  
 Publisher: ACM

 Full text available: pdf(108.80 KB) [Additional Information: full citation, abstract, references, cited by, index terms](#)

The day is approaching when most of our common transactions may be information-rich, but first an extensive supporting infrastructure must be developed in three areas: devices, networking, and trust.

[Trace A Pt Find out wh cell phone i type in the i](#)  
[www.cdnlab.org](http://www.cdnlab.org)

44 [Risks to the public in computers and related systems](#)

Peter G. Neumann

March 2003 ACM SIGSOFT Software Engineering Notes, Volume 28 Issue 2

Publisher: ACM

Full text available: pdf(221.43 KB) Additional Information: full citation, cited by

45 [Report of the national workshop on internet voting: issues and research agenda](#)

C. D. Mote, Jr.

May 2000 dg.o '00: Proceedings of the 2000 annual national conference on Digital government research

Publisher: Digital Government Research Center

Full text available: pdf(539.99 KB) Additional Information: full citation, abstract

As use of the Internet in commerce, education and personal communication has become common, the question of Internet voting in local and national elections naturally arises. In addition to adding convenience and precision, some believe that Internet ...

46 [PicoDBMS: Scaling down database techniques for the smartcard](#)

Philippe Pucheral, Luc Bouganim, Patrick Valduriez, Christophe Bobineau

September 2001 The VLDB Journal — The International Journal on Very Large Data Bases, Volume 10 Issue 2-3

Publisher: Springer-Verlag New York, Inc.

Full text available: pdf(259.03 KB) Additional Information: full citation, abstract, references, cited by, index terms

Smartcards are the most secure portable computing device today. They have been used successfully in applications involving money, and proprietary and personal data (such as banking, healthcare, insurance, etc.). As smartcards get more powerful (with ...

**Key words:** Atomicity, Durability, Execution model, PicoDBMS, Query optimization, Smartcard applications, Storage model

47 [Risks to the public](#)

Peter G. Neumann

May 2005 ACM SIGSOFT Software Engineering Notes, Volume 30 Issue 3

Publisher: ACM


Full text available: pdf(177.87 KB) Additional Information: full citation, abstract, index terms

Edited by Peter G. Neumann (Risks Forum Moderator and Chairman of the ACM Committee on Computers and Public Policy), plus personal contributions by others, as indicated. Opinions expressed are individual rather than organizational, and all of the usual ...

48 [MediaAlert - a broadcast video monitoring and alerting system for mobile users](#)

Bin Wei, Bernard Renger, Yih-Farn Chen, Rittwik Jana, Huale Huang, Lee Begeja, David Gibbon, Zhu Liu, Behzad Shahraray


June 2005 MobiSys '05: Proceedings of the 3rd international conference on Mobile systems, applications, and services  
 Publisher: ACM

Full text available:  pdf(593.10 KB) Additional Information: full citation, abstract, references, cited by, index terms

We present a system for automatic monitoring and timely dissemination of multimedia information to a range of mobile information appliances based on each user's interest profile. Multimedia processing algorithms detect and isolate relevant video segments ...


Key words: alerting, automatic speech recognition (ASR), content adaptation, content repurposing, mobile devices, multimedia messaging, multimedia processing, news monitoring, notification, service platform

#### 49 [Seeing, hearing, and touching: putting it all together](#)

 Brian Fisher, Sidney Fels, Karon MacLean, Tamara Munzner, Ronald Rensink  
 August 2004 SIGGRAPH '04: ACM SIGGRAPH 2004 Course Notes  
 Publisher: ACM

Full text available:  pdf(20.64 MB) Additional Information: full citation, cited by

#### 50 [Protecting applications with transient authentication](#)


 Mark D. Corner, Brian D. Noble  
 May 2003 MobiSys '03: Proceedings of the 1st international conference on Mobile systems, applications and services  
 Publisher: ACM

Full text available:  pdf(294.40 KB) Additional Information: full citation, abstract, references, cited by


How does a machine know who is using it? Current systems authenticate their users infrequently, and assume the user's identity does not change. Such *persistent authentication* is inappropriate for mobile and ubiquitous systems, where associations ...


#### 51 [Perils and pitfalls of practical cybercommerce](#)

 Nathaniel S. Borenstein  
 June 1996 Communications of the ACM, Volume 39 Issue 6  
 Publisher: ACM

Full text available:  pdf(465.63 KB) Additional Information: full citation, references, cited by, index terms, review

#### 52 [NETKIT: a software component-based approach to programmable networking](#)

 Geoff Coulson, Gordon Blair, David Hutchison, Ackbar Joolia, Kevin Lee, Jo Ueyama, Antonio Gomes, Yimin Ye  
 October 2003 ACM SIGCOMM Computer Communication Review, Volume 33 Issue 5  
 Publisher: ACM

Full text available:  pdf(316.64 KB) Additional Information: full citation, abstract, references, cited by, index terms

While there has already been significant research in support of openness and



programmability in networks, this paper argues that there remains a need for generic support for the integrated development, deployment and management of programmable networking ...

Key words: components, middleware, programmable networking, reflection

### 53 Risks to the public



Peter G. Neumann

July 2005 ACM SIGSOFT Software Engineering Notes, Volume 30 Issue 4

Publisher: ACM

Full text available: pdf(151.77 KB) Additional Information: full citation, abstract, index terms

Edited by Peter G. Neumann (Risks Forum Moderator and Chairman of the ACM Committee on Computers and Public Policy), plus personal contributions by others, as indicated. Opinions expressed are individual rather than organizational, and all of the usual ...

### 54 Securing Mobile Appliances: New Challenges for the System Designer

Anand Raghunathan, Srivaths Ravi, Sunil Hattangady, Jean-Jacques Quisquater

March 2003 DATE '03: Proceedings of the conference on Design, Automation

and Test in Europe - Volume 1, Volume 1

Publisher: IEEE Computer Society

Additional Information: full citation, abstract,

Full text available: pdf(157.28 KB); Publisher Site

references, cited by, index terms

As intelligent electronic systems pervade all aspects of our lives, capturing, storing, and communicating a wide range of sensitive and personal data, security is emerging as a critical concern that must be addressed in order to enable several current ...

### 55 Understanding human reactivities and relationships: an excerpt from Leonardo's laptop



Ben Shneiderman

September 2002 Interactions, Volume 9 Issue 5

Publisher: ACM

Full text available: pdf(426.22 KB); html(65.97 KB) Additional Information: full citation, abstract, index terms

"These notes reveal the intimate tie in Leonardo's thinking between... phenomena in general and the need to put such information to practical use." < BR> --- A. Richard Turner, *Inventing Leonardo*, 1994, p 184

### 56 Component-based interchangeable cryptographic architecture for securing wireless connectivity in Java<sup>TM</sup> applications

Johnny Li-Chang Lo, Judith Bishop

September 2003 SAI CSI T '03: Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology

Publisher: South African Institute for Computer Scientists and Information Technologists

Full text available:  pdf(147.85 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

The development of Java based wireless applications presents challenges such as securing communication and authentication between mobile devices and a server. It is acknowledged that cryptography is commonly used to secure network communications and ...


Keywords: component, cryptography, general packet radio services, global system for mobile applications, mobile devices, protocols, separation of concerns, wireless application protocol, wireless transport layer security

## 57 [What is money?](#)

Ray Byler

April 2004 MSCCC '04: Proceedings of the 2nd annual conference on Mid-south college computing

Publisher: Mid-South College Computing Conference

Full text available:  pdf(204.52 KB) Additional Information: [full citation](#), [abstract](#), [references](#)

Do you really know what money is? Most of the money that exists today doesn't exit as greenbacks in someone's wallet or gold in a Vault, but as 1's and 0's in some computer. What exactly is money then, and how does digital money differ from "real" money? ...

## 58 [Proceedings of the 2004 conference on Asia South Pacific design automation: electronic design and solution fair: electronic design and solution fair](#)

Masaharu Imai

January 2004 proceeding

Publisher: IEEE Press

Additional Information: [full citation](#), [abstract](#)

It is my pleasure and honor, on behalf of the Organizing Committee, to welcome you to the Asia and South Pacific Design Automation Conference 2004 (ASP-DAC 2004), a sister conference of DAC, DATE, and ICCAD. ASP-DAC 2004 will be held at Pacifico Yokohama, ...

Results 41 - 58 of 58

Result page: << [previous](#) [1](#) [2](#) [3](#)

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2008 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  [Adobe Acrobat](#)  [QuickTime](#)  [Windows Media Player](#)  [Real Player](#)


[Home](#) | [Login](#) | [Logout](#) | [Account Information](#) | [Alerts](#) | [Purchase Help](#)

Welcome United States Patent and Trademark Office

[Search Results](#)
[BROWSE](#)
[SEARCH](#)
[IEEE Xplore GUIDE](#)

Results for "((aim &lt;and&gt; pin &lt;and&gt; (authenticate &lt;or&gt; identify &lt;or&gt; validate) &lt;and&gt;...)"

Your search matched 0 of 1745737 documents.

A maximum of 100 results are displayed. 25 to a page, sorted by Relevance in Descending order.


[Search Options](#)
[View Session History](#)
[New Search](#)
[Key](#)

IEEE JNL	IEEE Journal or Magazine
IET JNL	IET Journal or Magazine
IEEE CXP	IEEE Conference Proceeding
IET CXP	IET Conference Proceeding
IEEE STD	IEEE Standard

Modify Search

((aim &lt;and&gt; pin &lt;and&gt; (authenticate &lt;or&gt; identify &lt;or&gt; validate) &lt;and&gt;... private key)


☐ Check to search only within this results set

Display Format:



Citation



Citation &amp; Abstract

[IEEE/IEE](#)
[Books](#)
[Educational Courses](#)

IEEE/IEE Journals, transactions, letters, magazines, conference proceedings, and standards.

[view selected items](#)
[Select All](#) [Deselect All](#)

No results were found.

Please edit your search criteria and try again. Refer to the Help pages if you need assistance revising your search

[Help](#) [Contact](#)
[Copy](#)

Powered by




[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)

 Search: ☒ The ACM Digital Library ☐ The Guide  
 ('smart and card' and 'private and key' and PIN and atm)

**THE ACM DIGITAL LIBRARY**


('smart and card' and 'private and key' and PIN and atm)

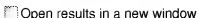
Terms used: 'smart card' 'private key' PIN atm

Found 21 of

Sort results by relevance


 Refine these results with [Advance Search](#)

Display results expanded form

Try this search in [The ACM Guide](#)

Results 1 - 20 of 21

Result page: 1 2

**1 [Smart Cards and Biometrics: The cool way to make secure transactions](#)**

David Corcoran, David Sims, Bob Hillhouse

March 1999 Linux Journal, Volume 1999 Issue 59es

Publisher: Specialized Systems Consultants, Inc.

Full text available: [html\(22.95 KB\)](#) [Additional Information: full citation, index terms](#)[Ads by Google](#)
 Comparison Co  
 Web based dec  
 making provide  
 ease and collab  
 www.enventhainc.c

**2 [Muscle Flexes Smart Cards into Linux](#)**

David Corcoran

August 1998 Linux Journal, Volume 1998 Issue 52es

Publisher: Specialized Systems Consultants, Inc.

Full text available: [html\(16.89 KB\)](#) [Additional Information: full citation, abstract, index terms](#)
 The newest kind of card for your pocketbook offers better security for the  
 information it holds

 Easy Decision  
 Fast Decision T  
 Software See E  
 Free Download  
 www.SimultLazio.co

**3 [Distributed PIN verification scheme for improving security of mobile devices](#)**

Jian Tang, Vagan Terziyan, Jari Veijalainen

April 2003 Mobile Networks and Applications, Volume 8 Issue 2

Publisher: Kluwer Academic Publishers

 Full text available: [pdf\(299.43 KB\)](#) [Additional Information: full citation, abstract, references, cited by, index terms](#)

 The main driving force for the rapid acceptance rate of small sized mobile devices  
 is the capability to perform e-commerce transactions at any time and at any  
 place, especially while on the move. There are, however, also weaknesses of this  
 type of e-commerce, ...

Keywords: measure, mobile device, probability, risks, security, uncover

 Research MIS  
 Your Guide to E  
 Schools & Mgm  
 Systems Certifi  
 AllBusiness Schools


 Decision Supp  
 System  
 Decision Suppc  
 System See 5 C  
 Offers at a Free  
 www.hopkinding.co

**4 [Privacy and security threat analysis of the federal employee personal identity verification \(PIV\) program](#)**

Paul A. Karger

July 2006 SOUPS '06: Proceedings of the second symposium on Usable privacy and

security  
Publisher: ACM

Full text available:  pdf(113.11 KB) Additional Information: full citation, abstract, references, index terms

This paper is a security and privacy threat analysis of new Federal Information Processing Standard for Personal Identity Verification (FIPS PUB 201). It identifies some problems with the standard, and it proposes solutions to those problems, using standardized ...


Key words: personal identification, privacy, smart cards

## 5 [Spy-resistant keyboard: more secure password entry on public touch screen displays](#)

Desney S. Tan, Pedram Keyani, Mary Czerwinski

November 2005 OZCHI '05: Proceedings of the 19th conference of the computer-human interaction special interest group (CHISIG) of Australia on Computer-human interaction: citizens online: considerations for today and the future


Publisher: Computer-Human Interaction Special Interest Group (CHISIG) of Australia

Full text available:  pdf(454.44 KB) Additional Information: full citation, abstract, references

Current software interfaces for entering text on touch screen devices mimic existing mechanisms such as keyboard typing or handwriting. These techniques are poor for entering private text such as passwords since they allow observers to decipher what ...


Key words: input technique, keyboard, password, selective attention, touch screen, visual search

## 6 [What is your husband's name?: sociological dimensions of internet banking authentication](#)

 Supriya Singh, Anuja Cabraal, Gabriele Hermansson

November 2006 OZCHI '06: Proceedings of the 20th conference of the computer-human interaction special interest group (CHISIG) of Australia on Computer-human interaction: design: activities, artefacts and environments


Publisher: ACM

Full text available:  pdf(205.49 KB) Additional Information: full citation, abstract, references, index terms

First order authentication of the privacy and security of Internet banking rests mainly on distinctive user names and passwords. Our qualitative study of banking, security and privacy shows it is common for married and de facto couples in Australia to ...


Key words: Australia, Internet banking, authentication, qualitative research, security design, sociological dimensions

## 7 [Password sharing: implications for security design based on social practice](#)

 Supriya Singh, Anuja Cabraal, Catherine Demosthenous, Gunela Astbrink, Michele Furlong

April 2007 CHI '07: Proceedings of the SIGCHI conference on Human factors in computing systems

Publisher: ACM

Full text available:  pdf(118.90 KB) [Additional Information: full citation, abstract, references, index terms](#)

Current systems for banking authentication require that customers not reveal their access codes, even to members of the family. A study of banking and security in Australia shows that the practice of sharing passwords does not conform to this requirement. ...

Keywords: Australia, UCD, banking, security, sharing passwords, social and cultural centered design

## 8 [Kimono: kiosk-mobile phone knowledge sharing system](#)



Albert Huang, Kari Pulli, Larry Rudolph

December 2005 MUM '05: Proceedings of the 4th international conference on Mobile and ubiquitous multimedia

Publisher: ACM

Full text available:  pdf(283.85 KB) [Additional Information: full citation, abstract, references](#)

The functionality of an information kiosk can be extended by allowing it to interact with a smartphone, as demonstrated by the Kimono system, and the user interface can be greatly simplified by "associations" between pieces of information. A kiosk provides ...


## 9 [At home with the technology: an ethnographic study of a set-top-box trial](#)



Jon O'Brien, Tom Rodden, Mark Rouncefield, John Hughes

September 1999 ACM Transactions on Computer-Human Interaction (TOCHI), Volume 6 Issue 3

Publisher: ACM

Full text available:  pdf(439.27 KB) [Additional Information: full citation, references, cited by, index terms, review](#)

Keywords: coordination and collaboration, domestic environment, ethnography, evaluation, interactive devices

## 10 [Risks to the public](#)



Peter G. Neumann

January 2006 ACM SIGSOFT Software Engineering Notes, Volume 31 Issue 1

Publisher: ACM

Full text available:  pdf(139.10 KB) [Additional Information: full citation, abstract, index terms](#)

Edited by Peter G. Neumann (Risks Forum Moderator and Chairman of the ACM Committee on Computers and Public Policy), plus personal contributions by others, as indicated. Opinions expressed are individual rather than organizational, and all of the usual ...



## 11 [Payments and banking with mobile personal devices](#)



Amir Herzberg


May 2003 Communications of the ACM, Volume 46 Issue 5

Publisher: ACM

Full text available:  pdf(152.82 KB)  html(31.60 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#), [review](#)


Mobile devices enable secure, convenient authorization of e-banking, retail payment, brokerage, and other types of transactions.

12 [SmartSiren: virus detection and alert for smartphones](#)

 Jerry Cheng, Starsky H.Y. Wong, Hao Yang, Songwu Lu

June 2007 MobiSys '07: Proceedings of the 5th international conference on Mobile systems, applications and services


Publisher: ACM

Full text available:  pdf(534.00 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Smartphones have recently become increasingly popular because they provide "all-in-one" convenience by integrating traditional mobile phones with handheld computing devices. However, the flexibility of running third-party softwares also leaves the smartphones ...


Key words: alert, privacy, security, smartphone, virus detection

13 [Information-rich commerce at a crossroads: business and technology adoption requirements](#)

 Robert G. Fichman, Mary J. Cronin


September 2003 Communications of the ACM, Volume 46 Issue 9

Publisher: ACM

Full text available:  pdf(108.80 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#)

The day is approaching when most of our common transactions may be information-rich, but first an extensive supporting infrastructure must be developed in three areas: devices, networking, and trust.

14 [Risks to the public in computers and related systems](#)

 Peter G. Neumann

March 2003 ACM SIGSOFT Software Engineering Notes, Volume 28 Issue 2

Publisher: ACM

Full text available:  pdf(221.43 KB) Additional Information: [full citation](#), [cited by](#)

15 [RFID and the end of cash?](#)

 Ian Angell, Jan Kietzmann

December 2006 Communications of the ACM, Volume 49 Issue 12

Publisher: ACM

Full text available:  pdf(965.22 KB)  html(29.48 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

RFID-embedded money is likely to mean the end of anonymous transactions and with it one of the last bastions of personal anonymity.


16 [Audio-visual multimodal fusion for biometric person authentication and liveness verification](#)

Girija Chetty, Michael Wagner

April 2006 MMUI '05: Proceedings of the 2005 NICTA-HCSNet Multimodal

User Interaction Workshop - Volume 57, Volume 57

Publisher: Australian Computer Society, Inc.

Full text available:  [pdf\(719.65 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

In this paper we propose a multimodal fusion framework based on novel face-voice fusion techniques for biometric person authentication and liveness verification. Checking liveness guards the system against spoof/replay attacks by ensuring that the biometric ...

Key words: biometric authentication, liveness verification, multimodal fusion


17 [Risks to the public](#)



Peter G. Neumann

May 2005 ACM SIGSOFT Software Engineering Notes, Volume 30 Issue 3

Publisher: ACM

Full text available:  [pdf\(177.87 KB\)](#) Additional Information: [full citation](#), [abstract](#), [index terms](#)

Edited by Peter G. Neumann (Risks Forum Moderator and Chairman of the ACM Committee on Computers and Public Policy), plus personal contributions by others, as indicated. Opinions expressed are individual rather than organizational, and all of the usual ...

18 [Seeing, hearing, and touching: putting it all together](#)



Brian Fisher, Sidney Fels, Karon MacLean, Tamara Munzner, Ronald Rensink

August 2004 SIGGRAPH '04: ACM SIGGRAPH 2004 Course Notes

Publisher: ACM

Full text available:  [pdf\(20.64 MB\)](#) Additional Information: [full citation](#), [cited by](#)


19 [Perils and pitfalls of practical cybercommerce](#)



Nathaniel S. Borenstein

June 1996 Communications of the ACM, Volume 39 Issue 6

Publisher: ACM

Full text available:  [pdf\(465.63 KB\)](#) Additional Information: [full citation](#), [references](#), [cited by](#), [index terms](#), [review](#)

20 [Risks to the public](#)




Peter G. Neumann

July 2005 ACM SIGSOFT Software Engineering Notes, Volume 30 Issue 4

Publisher: ACM



Full text available:  pdf(151.77 KB) **Additional Information:** full citation, abstract, index terms

Edited by Peter G. Neumann (Risks Forum Moderator and Chairman of the ACM Committee on Computers and Public Policy), plus personal contributions by others, as indicated. Opinions expressed are individual rather than organizational, and all of the usual ...

Results 1 - 20 of 21

Result page: 1 2

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2008 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  Adobe Acrobat  QuickTime  Windows Media Player  Real Player


[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)

 Search: The ACM Digital Library The Guide  
 ('smart and card' and 'private and key' and PIN and atm)


THE ACM DIGITAL LIBRARY

[Feedback](#)

('smart and card' and 'private and key' and PIN and atm)

Found 21 of 238,786

Terms used: 'smart card' 'private key' PIN atm

Sort results  
by

relevance

[Save results to a Binder](#)Display  
results

expanded form

[Open results in a new window](#)Refine these results with [Advanced Search](#)Try this search in [The ACM Guide](#)

Results 21 - 21 of 21

Result page: [<<](#) [previous](#) [1](#) [2](#)21 [What is money?](#)

Ray Byler

April 2004 MSCCC '04: Proceedings of the 2nd annual conference on Mid-south college computing

Publisher: Mid-South College Computing Conference

Full text available: pdf(204.52 KB) [Additional Information: full citation, abstract, references](#)

Do you really know what money is? Most of the money that exists today doesn't exit as greenbacks in someone's wallet or gold in a Vault, but as 1's and 0's in some computer. What exactly is money then, and how does digital money differ from "real" money? ...

Ads by Google

NI Graphical  
Programming  
Powerful, Intuitive  
Programming w/  
LabVIEW- Online  
Tutorials & Evals.

[www.ni.com](#)
[Linear Programming](#)

Excel  
Easy Modeling, Large  
Scale LP, MIP,  
Download Free Trial  
Version

[www.covel.com](#)
[Embedded C/C++](#)

Training  
Hardware Interfacing In  
C/C++ 1-4 Days Hands  
On, Your Site  
[No/Insite.com](#)

[Teach programming to  
kids](#)

Curriculum, tutorials,  
books, help Download  
now for free!

[www.proboards.com](#)

Results 21 - 21 of 21

Result page: << previous 1 2

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2008 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  Adobe Acrobat  QuickTime  Windows Media Player  Real Player

Web Images Maps News Shopping Gmail more ▾

Sign in

Google

atm "PIN encryption key" "private key" issuer

Search

Advanced Search  
Preferences

Web

Results 1 - 10 of about 60 for atm "PIN encryption key" "private key" issuer. (0.32 seconds)

Did you mean: atm "PIN encryption key" "private key" *issues*

[DOC] [ISO/IEC TC /SC N](#)

File Format: Microsoft Word - [View as HTML](#)

Card Issuers (CI) – Financial institutions that issue PIN enabled cards for use in ATM and POS environments. Direct Processors (DP) – Members or sponsored ...

[www.x9.org/standards/free/TG-3\\_final\\_2006.doc](#) - [Similar pages](#)

[PDF] [Payment Card Industry PIN Security Requirements](#)

File Format: PDF/Adobe Acrobat - [View as HTML](#)

entry to the card issuer, the encrypted PIN block format. must comply with ISO 9564–1 format 0 ... used for encryption zones where the PIN encryption key is ...

[https://partnernetwork.visa.com/vpni/global/retrieve\\_document.do?documentRetrieveId=95](#) - [Similar pages](#)

[PDF] [Cryptographic processors - a survey](#)

File Format: PDF/Adobe Acrobat - [View as HTML](#)

forcing PIN re-issue. The designers produced a transaction. of the following form, warning that it ..... returned encrypted under a PIN Encryption Key (PEK) ...

[www.cl.cam.ac.uk/techreports/UCAM-CL-TR-641.pdf](#) - [Similar pages](#)

[PDF] [Chunghwa Telecom Co., Ltd. HICOS PKI Smart Card Security Policy](#)

File Format: PDF/Adobe Acrobat - [View as HTML](#)

The card manager security domain corresponds to the card issuer security ..... The private-key, which is retained securely within the PKI container, is used ...

[csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp614.pdf](#) - [Similar pages](#)

[Pin creation system and method invention](#)

While this may be feasible if the consumer is at an ATM, bank branch or similar ... assigned by the card issuer or previously selected by the user). ...

[www.freshpatents.com/Pin-creation-system-and-method-dr20071206ptan20070282756.php?type=description - 43k](#) - [Cached](#) - [Similar pages](#)

[PDF] [STANDARD 70-5](#)

File Format: PDF/Adobe Acrobat - [View as HTML](#)

Recommendations for Switches and the Issuer or Authorizing Host .... Key Encryption Key should never be used as a PIN Encryption Key. ...

[www.nyce.net/resources/pdf/BestPracticesforPointofSaleSecurity.pdf](#) - [Similar pages](#)

[PDF] [Automated Analysis of Security APIs Amerson H. Lin](#)

File Format: PDF/Adobe Acrobat - [View as HTML](#)

To authenticate the customer present at the ATM, banks issue a PIN to ..... Although we do not have access to the PIN encryption key, any trial PIN can be ...

[sdg.csail.mit.edu/pubs/theses/amerson-masters.pdf](#) - [Similar pages](#)

[PDF] [Sun Crypto Accelerator 6000 Board User's Guide](#)

File Format: PDF/Adobe Acrobat - [View as HTML](#)

ATM card at a different bank than the one that issued the card. At the transaction,. the PIN comes in encrypted using a PIN encryption key (PEK) specified ...

[dlc.sun.com/pdf/819-5536-11/819-5536-11.pdf](#) - Similar pages

[PDF] **Exploiting S/390 Hardware Cryptography with Trusted Key Entry**

File Format: PDF/Adobe Acrobat

Digital signatures - signing a message with the private key. .... PIN encryption key - This is a 128-byte unidirectional key used for PIN . translation. ...

[www.redbooks.ibm.com/redbooks/pdfs/sg245455.pdf](#) - Similar pages

[PDF] **SG244579**

File Format: PDF/Adobe Acrobat

More information about CDMF can be found in the March 1994 issue of the IBM ..... PIN encryption key - a 128-byte unidirectional key used for PIN ...

[www.redbooks.ibm.com/redbooks/pdfs/sg244579.pdf](#) - Similar pages

Did you mean to search for: [atm "PIN encryption key" "private key" issues](#)

1 2 [Next](#)

---

atm "PIN encryption key" "private ke"

[Search within results](#) | [Language Tools](#) | [Search Tips](#) | [Dissatisfied? Help us improve](#) | [Try Google Experimental](#)

---

©2008 Google - [Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)


[Home](#) | [Login](#) | [Logout](#) | [Access Information](#) | [Alerts](#) | [Purchase for](#)

Welcome Unpublished Patent and Trademark Office

[Search Results](#)
[BROWSE](#)
[SEARCH](#)
[IEEE Xplore GUIDE](#)

Results for "((((be &lt;or&gt; 'identity based') &lt;and&gt; 'smart card')&lt;in&gt;metadata)) &lt;and&gt; (...)"

Your search matched 3 of 1748191 documents.

A maximum of 100 results are displayed. 25 to a page, sorted by Relevance in Descending order.


[Search Options](#)
[View Session History](#)
[New Search](#)
[Key](#)

IEEE JNL IEEE Journal or Magazine  
 IET JNL IET Journal or Magazine  
 IEEE CFP IEEE Conference Proceeding  
 IET CFP IET Conference Proceeding  
 IEEE STD IEEE Standard

Modify Search

(((((be &lt;or&gt; 'identity based') &lt;and&gt; 'smart card')&lt;in&gt;metadata)) &lt;and&gt; (pyr &gt;= 1950) &lt;


☐ Check to search only within this results set

Display Format



Citation



Citation &amp; Abstract

[IEEE/ET](#)
[Books](#)
[Educational Courses](#)

Practical applied content provided by GlobalSpec to explain, illustrate and promote technologies. Not reviewed

[Select All](#) [Deselect All](#)

- Efficient identification and signature schemes  
 Ohta, K.;  
[Electronics Letters](#)  
 Volume 24, Issue 2, 21 Jan. 1988 Page(s):115 - 116  
[AbstractPlus](#) | Full Text: PDF(224 KB) IET JNL
- The ID-based non-interactive group communication key sharing scheme using smart cards  
 Sakakibara, H.; Seki, K.; Okada, K.; Matsushita, Y.;  
[Network Protocols, 1994. Proceedings, 1994. International Conference on](#)  
 25-28 Oct. 1994 Page(s):91 - 98  
 Digital Object Identifier 10.1109/CNP.1994.344372  
[AbstractPlus](#) | Full Text: PDF(580 KB) IEEE CFP  
[Rights and Permissions](#)
- Remote password authentication with smart cards  
 Chang, C.-C.; Wu, T.-C.;  
[Computers and Digital Techniques, IEEE Proceedings](#)  
 Volume 138, Issue 3, May 1991 Page(s):165 - 168  
[AbstractPlus](#) | Full Text: PDF(236 KB) IET JNL

Indexed by


[Help](#) [Contact](#)
[© Copy](#)


[Home](#) | [Login](#) | [Logout](#) | [Access Information](#) | [Alerts](#) | [Purchase Help](#)

Welcome (United States Patent and Trademark Office)

[Search Results](#)
[BROWSE](#)
[SEARCH](#)
[IEEE Xplore GUIDE](#)

Results for "(((atm &lt;and&gt; pin &lt;and&gt; (be &lt;or&gt; 'identity based'))&lt;in&gt;metadata)) &lt;and&gt;..."

Your search matched 0 of 1748191 documents.

A maximum of 100 results are displayed, 25 to a page, sorted by Relevance in Descending order.


[Search Options](#)
[View Session History](#)
[New Search](#)

Key

IEEE JNL	IEEE Journal or Magazine
IET JNL	IET Journal or Magazine
IEEE CONF	IEEE Conference Proceeding
IET CONF	IET Conference Proceeding
IEEE STD	IEEE Standard

Query Search

(((atm &lt;and&gt; pin &lt;and&gt; (be &lt;or&gt; 'identity based'))&lt;in&gt;metadata)) &lt;and&gt; (pyr &gt;= 199)

☐ Check to search only within this results set

Display Format



Citation



Citation &amp; Abstract

[IEEE/ET](#)
[Books](#)
[Educational Courses](#)

IEEE/ET journals, transactions, letters, magazines, conference proceedings, and standards.

Select All Deselect All

No results were found.

Please edit your search criteria and try again. Refer to the Help pages if you need assistance revising your search

[Help](#) [Contact](#)

© 2005




[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)

 Search: ☒ The ACM Digital Library ☐ The Guide  
 (ibe and pin)


THE ACM DIGITAL LIBRARY

Feedback

 (ibe and pin)  
 Terms used: [ibe](#) [pin](#)

Found 5 of 20

Sort results by relevance

☒ Save results to a Binder

 Refine these results with [Advanced Search](#)

Display results expanded form

☐ Open results in a new window
Try this search in [The ACM Guide](#)

Results 1 - 5 of 5

### 1 [Card shark and thespis: exotic tools for hypertext narrative](#)

Ads by Google



Mark Bernstein

 September 2001 [HYPERTEXT '01: Proceedings of the twelfth ACM conference on Hypertext and Hypermedia](#)

Publisher: ACM

 Full text available: pdf(226.42 KB) [Additional Information: full citation, abstract, references, cited by, index terms](#)

Card Shark and Thespis are two newly-implemented hypertext systems for creating hypertext narrative. Both systems depart dramatically from the tools currently popular for writing hypertext fiction, and these departures may help distinguish between the ...

Keyw ords: fiction, hypertext systems, narrative, storyspace

[Book Publishing Services](#)  
 We Discover & Make  
 New Authors! Ret.  
 40% Royalties. For  
 More  
[www.TalePublishing.co](#)

[Be a Book Publisher](#)  
 Become a Book  
 Publisher It's Fast  
 Easy, Get Free  
 Publishing Info Now  
[www.BeAPublisher.com](#)

### 2 [A secure authentication and billing architecture for wireless mesh networks](#)

Yanchao Zhang, Yuguang Fang

October 2007 [Wireless Networks](#), Volume 13 Issue 5

Publisher: Kluwer Academic Publishers

 Full text available: pdf(501.79 KB) [Additional Information: full citation, abstract, references, index terms](#)

Wireless mesh networks (WMNs) are gaining growing interest as a promising technology for ubiquitous high-speed network access. While much effort has been made to address issues at physical, data link, and network layers, little attention has been paid ...

Keyw ords: authentication, billing, roaming, security, wireless mesh networks (WMNs)

[T-Shirt Fulfillment](#)  
 T-Shirt Fulfillment  
 templates Shopping  
 Carts, Screen Print  
[www.carechoprints.co](#)

### 3 [CMIFed: a presentation environment for portable hypermedia documents](#)


 Guido van Rossum, Jack Jansen, K. Sjoerd Mullender, Dick C. A. Bulterman  
 September 1993 [MULTIMEDIA '93: Proceedings of the first ACM international conference on Multimedia](#)

Publisher: ACM

 Full text available: pdf(175.93 KB) ps(867.94 KB) [Additional Information: full citation, references, cited by, index terms](#)

[E-Commerce Solutions](#)  
 Get Multiple Quotes  
 Your Order Custom  
 Designs Available  
[www.BuyersZone.com](#)



**Keywords:** CMIF, editing environment, heterogeneity, hypermedia, multimedia, portability, scheduling, synchronization

#### 4 [Novel wire density driven full-chip routing for CMP variation control](#)

Huang-Yu Chen, Szu-Jui Chou, Sheng-Lung Wang, Yao-Wen Chang

November 2007 ICCAD '07: Proceedings of the 2007 IEEE/ACM international conference on Computer-aided design

Publisher: IEEE Press

Full text available:  pdf(1.29 MB) **Additional Information:** [full citation](#), [abstract](#), [references](#)

As nanometer technology advances, the post-CMP dielectric thickness variation control becomes crucial for manufacturing closure. To improve CMP quality, dummy feature filling is typically performed by foundries after the routing stage. However, filling ...


#### 5 [FPGA interconnect planning](#)



Amit Singh, Malgorzata Marek-Sadowska

April 2002 SLI P '02: Proceedings of the 2002 international workshop on System-level interconnect prediction

Publisher: ACM

Full text available:  pdf(144.62 KB) **Additional Information:** [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#)

We present an FPGA interconnect planning methodology based on the empirical measure known as Rent's Rule[8]. We show that allocation of wire segment lengths during the FPGA architecture planning phase can be improved by taking into account interconnect ...

Results 1 - 5 of 5

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2008 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  Adobe Acrobat  QuickTime  Windows Media Player  Real Player